Medical Law International, 2004, Vol. 6, pp. 73–86
0968-5332/04 $10

WHEN IS PERSONAL DATA RENDERED ANONYMOUS? INTERPRETING RECITAL 26 OF DIRECTIVE 95/46/EC

DERYCK BEYLEVELD, PROFESSOR OF JURISPRUDENCE AND
DAVID M.R. TOWNEND, LECTURER IN LAW

*University of Sheffield**

INTRODUCTION

Anonymisation is seen in scientific research as the chief protection of the rights of individuals who are the subjects of research. Guarantees of protection for the interests of research subjects are vital, especially in medical research. Without assurances of privacy and protection of other fundamental rights and freedoms, it is not just participation in research that is threatened, but the basis of trust throughout healthcare and health development is undermined. It is a real danger that, without appropriate safeguards engendering trust in researchers and healthcare professionals, individuals will not come forward for diagnosis and treatment. Therefore, creating the correct legal framework to ensure that confidence in doctors and researchers is vital. Yet the extent and value of anonymisation is still uncertain. Indeed, in England the dominant view is that protection of research subjects concerns *only* the immediate protection of identity of the individual, and that the research subject has no greater need or call on protection than a removal of identifiers from the personal data.

The European Directive on Data Protection (95/46/EC), we will argue, goes much further than the English view in its requirements for anonymisation. Further, we will show that the necessary protection of patients' fundamental rights and freedoms requires a full protection of their sensibilities as well as their identity. We will use three sets of questions to make the argument. First, however, the Directive's requirements must be understood.

The governing aim of Directive 95/46/EC on data protection is:

> to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. (Article 1.1)

*This paper is based upon a paper delivered at the 14th World Congress on Medical Law, Maastricht, August 2002.

For the purposes of the Directive, personal data is:

> any information relating to an identified or identifiable natural person ("data subject"). (Article 2(a))

In accordance with this, Recital 26 explains that:

> the principles of protection[1] must apply to any information concerning an identified or identifiable individual

but goes on to say that:

> the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable . . . .

However, it is not clear when data is to be regarded as having been rendered anonymous, and that is the heart of the problem. It might seem that the only issue is when the data subject is to be considered no longer identifiable. If that were the case, then Article 2(a) specifies that:

> an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

and, in relation to which, Recital 26 states that:

> to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used[2] by either the controller or by any other person to identify the said person . . . [and] codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible.

However, Article 2(b) specifies that processing of personal data is "any operation or set of operations which is performed on personal data". So this broad definition of processing means that anonymisation of personal data is processing of personal data, and Recital 26 is clear that the principles of protection apply to personal data *before* it is rendered anonymous. This also raises the question whether the processing of *non-personal* information generated from data obtained as personal data is, at least in some contexts, to be considered processing of personal data, hence subject to applicable principles of protection and not "anonymous".

Those then are the basic principles of the Directive in this area. To

give further focus to this issue, we will specifically consider the following questions.

(1) *A*, a doctor who is also a medical researcher, obtains data related to a person's health in personal form for medical treatment of that person. Without informing the patient of this, *A* intends to use information contained in this data for genetic research. While *A* will retain the original data in personal form, *A* will take information from it that *A* will keep in non-personal form (i.e., the patient (data subject) will not be identifiable from the information by itself) and *A* will only process this "non-personal" information for genetic research.

From this scenario, the following questions arise. If *A* so processes the information, is *A* in breach of any of the data protection principles? In short, is *A's* processing of this non-personal information processing of data rendered anonymous for the purposes of Recital 26? In particular, must *A* comply with Article 10, 11.1, 7 and 8 with respect to the processing of personal for genetic research?[3]

(2) In the second scenario, we introduce *B*, a data base company that wishes to compile aggregated data on prescriptions given to patients so that it can sell this information to pharmaceutical companies for the purposes of direct marketing of doctors. If *A* continues to hold the data originally obtained in personal form and passes non-personal information taken from it to data controller *B*, do any of the data protection principles apply to *B's* processing of the non-personal information abstracted from the personal data held by *A?*

(3) If scenarios (1) and (2) are altered so that *A* renders the original data non-personal (so that *no-one* can now identify the data subject from it directly or indirectly) before processing it for genetic research or passing any information it contained to *B* (the data no longer being required for the patient's treatment), do any of the data protection principles apply to *A's* or *B's* processing of what is now the non-personal information held by *A* or received by *B?*

There are those who maintain that the non-personal information processed in all three of these scenarios is data rendered anonymous so that the principles of protection do not apply to it.[4] We, however, will argue, on the basis of Articles 2(a), 2(b), 11.1 and 13.2 of the Directive, and Strasbourg jurisprudence on Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[5], that the processing of non-personal information is not necessarily beyond the scope of the principles of protection in any of the

three scenarios. In relation to scenarios (1) and (2), we contend, there is no difficulty squaring this with Recital 26 because the non-personal information in those scenarios is clearly personal data under the Directive. However, as our general analysis bears on scenario (3), it suggests that personal data can never be rendered beyond the scope of the principles of protection simply by rendering it non-personal *when* there is an identifiable *obtaining data controller and* the data subject has provided personal data for limited purposes only. This, however, requires Recital 26 to be given a constructive interpretation or to be declared not fully compatible with the operative provisions of the Directive. In any event, we conclude that it must be held that it is not legitimate for data controllers to render data non-personal in a way that would place subsequent processing of the data beyond the scope of the principles of protection when the data has been obtained for limited purposes.

Scenario (1)

Article 10 requires the data controller, *inter alia*, to inform the data subject of "the purposes of the processing for which the data are intended". Article 2(b) defines "processing of personal data" as "any operation or set of operations which is performed upon personal data, whether or not by automatic means". Thus, anonymisation (rendering personal data non-personal) is itself a process governed by the principles of protection. Hence, the data subject must be informed of "the purposes of the anonymisation for which the data are intended".

It might, however, be argued that this means only that the data subject must be informed of the purposes of anonymisation rather than of the intended purposes of processing after anonymisation. Whether or not this is so depends on whether or not the Directive operates with the view that to process information *contained in* personal data is to process the personal data even though the information being processed is not itself personal.

In relation to this, it is clear that the Directive considers the processing of non-personal information contained in personal data to be processing of personal data. This follows simply from Article 2(a), which defines personal data as any information that relates to an individual who can be identified directly or indirectly from the data. Since *A* surely knows that the non-personal information has been generated from the personal data *A* holds, *A* can still identify the data subject from whom the non-personal information was obtained.[6]

Scenario (2)

In this scenario, *A* retains personal data gathered from data subjects

(who were told about the purposes for which the information was gathered as required by Article 10: Article 10 information). *A* passes non-personal information contained in the personal data (derived-information) to *B* (in our example, *A* holds the full patient records and passes only the details of the medical conditions and prescribed drug therapies to *B*. What are *B*'s responsibilities under the data protection principles?

Recital 26 makes it clear that data remains personal data if the data subject is reasonably likely to be identifiable directly or indirectly by the controller *or any other person.* Consequently, it is personal data if the data subject is reasonably likely to be identifiable directly or indirectly by any person.[7] Hence, in scenario (2), the non-personal information in *B's* hands can, on no account, be considered "rendered anonymous" because *A* can still easily identify the data subject. Consequently, *B's* processing is governed by the information provided by *A* to the data subject (Article 10 information) and the conditions for lawful processing imposed on *A*.[8]

However, the question of whether *B's* processing is governed by the Article 10 information provided by *A* to the data subject must be distinguished from the question of whether *B* is liable for processing in accordance with this Article 10 information. Clearly, if *B* has received non-personal information (derived from the personal data: derived-information) then *B* will not be able to contact the data subject or subjects from whom this derived-information was obtained (at least directly). *B's* liability will be restricted to processing the derived-information in accordance with what *A* informs *B* about any limits placed on the purposes of the processing (*A*, surely, having a duty to inform *B* of any restrictions placed by the data subject on this processing).[9]

Scenario (3)

In this scenario, *A* renders the original data non-personal such that no-one can identify the data subject either directly or indirectly. The information that is disclosed by *A* to *B* appears to be no longer personal data because the personal data from which it was derived is now no longer personal data. The information, we might say, is information that has been extracted from personal data but is not information that is contained in personal data. Nevertheless there are both textual and theoretical reasons for thinking that non-personal information extracted from personal data but not contained in personal data can still be personal data for the purposes of the Directive.[10]

First, the purposes for which the non-personal information extracted from personal data are to be processed might very well be purposes for which the personal data is obtained (collecting and recording personal data being specifically cited in Article 2(b) as examples of processing of personal data and anonymisation of the data clearly being an act of

processing of the data). Hence, Article 10, in requiring the data subject to be informed of "the purposes of the processing for which the data are intended" directly requires the data subject to be informed of the purposes for which the non-personal information will be processed after anonymisation where they are known at the time of collection of the data from the data subject.

Secondly, Article 11.2, which exempts from Article 11.1:

> where, in particular for processing for statistical purposes . . . the provision of such information proves impossible or would involve a disproportionate effort or disclosure is expressly laid down by law

nevertheless requires that "Member States shall provide appropriate safeguards". In principle, processing for statistical purposes renders personal data, *in that processing*, non-personal. So, why must Member States still provide appropriate safeguards, unless the principles of protection continue to apply to the processing of information rendered non-personal in this context?

Thirdly,

> when data are . . . kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics

Article 13.2 allows an exemption *only* from Article 12 (the data subject's right of access to data and right to rectify, erase, or block data). Again, this exemption is subject to adequate legal safeguards. The direct implication is that there is no exemption from any requirements of the Directive, other than those of Article 12, in relation to processing that will occur after the data is rendered non-personal when this data was originally obtained in personal form simply on the basis that the information involved *will be* rendered non-personal before that processing occurs.

Fourthly, it is vital not to lose sight of the fact that the objective of the Directive is to protect fundamental rights and freedoms, and privacy in particular.

Some, including the UK Court of Appeal in the *Source Informatics* case,[11] seem to believe that the only interest that data subjects have in the use of personal data obtained for their medical treatment is in their treatment and in the concealment of their personal identities in the disclosure or other use of that data. Consequently, they hold that there can be no breach of any right to privacy in relation to this data if information contained in personal data is disclosed or used in a non-personal form (which covers scenarios (1) and (2) as well as scenario 3).

This view is presented with a serious difficulty, however. This is that the right to privacy under Article 8(1) of the European Convention on

Human Rights (ECHR) is not merely a right to concealment of one's personal identity in relation to sensitive personal data. For example, the right extends to a right to moral integrity (which, in certain aspects, also falls under the Article 9(1) ECHR right to freedom of conscience, thought and religion). Professor Jacques Velu argues that the right to respect for private life under Article 8.1 of the ECHR

> protects the individual against:
> 1. Attacks on his physical or mental integrity or his moral or intellectual freedom.
> 2. Attacks on his honour and reputation and similar torts.
> 3. The use of his name, identity or likeness.
> 4. Being spied upon, watched or harassed.
> 5. The disclosure of information protected by the duty of professional secrecy.[12]

Indeed, the Commission of the Council of Europe has declared that the

> scope of the right to respect for private life is such that it secures to the individual a sphere within which he can freely pursue the development and fulfilment of his personality.[13]

And, more recently, L.G. Loucaides concluded that case law under the ECHR

> has expounded and upheld the protection of privacy to such a degree that, for all practical purposes, the right of privacy has become a functional equivalent of a right of personality, potentially embracing all those constituent parts of the personality of the individual that are not expressly safeguarded by the European Convention.[14]

Now, rendering personal information non-personal is surely not by itself sufficient to preclude a violation of one's moral integrity. That this is so should be clear from contemplation of the idea that information on the menstrual cycles of Roman Catholic women, who have provided the information for their treatment, might be used for purposes of research into chemical contraceptives without offending their moral integrity merely because the information processed was first rendered non-personal. Clearly, if the privacy (*qua* moral integrity) of those with conscientious objections to contraception is to be respected they must, at the very least, be informed of such processing (if it is anticipated[15]) so that they might object, and it does not matter that the information processed (together with the personal data from which it is extracted) will first be rendered non-personal.

Whether or not the data subject conscientiously objects to

processing in a particular case is essentially a subjective matter. It follows that any processing of which the data subject is not informed might potentially be a matter of conscientious objection for a data subject, in which case processing will breach that data subject's privacy according to Article 8.1 ECHR. In such cases it might be possible to justify the breach of Article 8.1 if Article 8.2 ECHR can be satisfied. This will be so where:

> this is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

However, this cannot be portrayed as a matter of the principles of protection not applying, because the conditions imposed by Article 8.2 are part of the principles of protection. Thus, for example, the fact that there might be an Article 8.2 justification for processing for genetic research without informing the data subject (especially where the information used is first anonymised) cannot be portrayed as a matter of the principles of protection not applying.[16]

Consequently, our view is that, if the Directive is to be consistent with the right to privacy, the processing of data extracted from personal data from which the data subject is no longer identifiable cannot be considered to be necessarily wholly beyond the scope of the principles of protection.[17]

What then are we to make of Recital 26?

It is a simple rule of construction that an obligation must be possible to fulfil: that "ought" implies "can". So if data controllers cannot comply with the principles of protection they cannot reasonably be placed under a duty to do so. Thus, at least insofar as rendering data non-personal makes it impossible for data controllers to comply with the principles of protection, Recital 26 is well-inspired. However, the thrust of our analysis is that Recital 26, if it is to be consistent with the relevant operative provisions of the Directive, above all Article 1.1, then it must be interpreted so that data controllers who obtain data in personal form are not released from applicable principles of protection[18] in relation to processing that will only occur after this data is rendered non-personal. This is the case whether or not the data rendered non-personal is information contained in personal data or information extracted from personal data which is itself rendered non-personal before the processing

will occur. Furthermore, processing by data controllers who receive data in non-personal form will not necessarily be beyond the ambit of the principles of protection, at least where these data controllers have obtained the non-personal data, directly or indirectly from an identifiable data controller who held it in personal form. This is because the identifiable data controller was under obligation to comply with applicable principles of protection, so the information given to the data subjects should govern processing by those who receive non-personal information from this data controller. Indeed, insofar as data controllers receive non-personal information from data controllers who held the source data in personal form, they should, in principle, be able to comply with other principles as well by reference to the data controllers who hold or held the source data. Of course, in all of these situations, there may be considerable difficulty short of literal impossibility for the principles of protection to be complied with. But our analysis indicates that these cases are to be dealt with by exemptions within the principles of protection, not as cases of inapplicability of the principles of protection.

It follows, we suggest, that the only times that data rendered non-personal can be said to be beyond the scope of the principles of protection is where the data no longer has a history that can link it to an identifiable data controller who obtained the personal source data from the data subject or where it is known that the source data was given for unlimited purposes. In the first case the data will be beyond the ambit of the principles of protection simply because the principles of protection cannot be applied to it. In the second case, the data subject will, in effect, have waived any privacy right with respect to the data, consent to any (legitimate) use removing any privacy interest not already removed by rendering the information non-personal.

However, the first of these cases only applies to data that has already been "rendered anonymous". It does not apply in advance of the data being rendered anonymous. If privacy (Article 1.1) is to be protected, it is surely not permissible to use anonymisation deliberately to place data beyond the scope of the principles of protection (to make it impossible for them to be complied with). It follows, we suggest, that unless the data subject has given informed consent (or at least informed non-objection) to unlimited use of the personal data provided, it is not permissible for data controllers to render the data non-personal in a way that would prevent the principles of protection from having possible application (*unless* the data subject has been informed of the intention to anonymise *and its consequences*[19]).

The problem with Recital 26 is that, if its statement that "the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable" is given a very narrow interpretation, according to which data is rendered anonymous if

the data subject, *as such,* is no longer identifiable from the data (directly or indirectly) then it suggests that the principles of protection do not apply in scenario (3) at least. This, we have argued, is not compatible with the objective of the Directive to protect privacy.

Faced with this situation, one possibility is to declare Recital 26 to be incompatible with Article 1.1 of the Directive. This is perfectly possible, for, as the European Court of Justice has declared in the *Nilsson* case, recitals "cannot be relied on as a ground for derogating from the actual provisions of the act in question".[20] However, this should be a matter of last resort, which it might be possible to avoid by giving Recital 26 a broad constructive interpretation. This can be done by, for example, holding the data subject to be identifiable where, with respect to data known to have been extracted from personal data (narrowly defined), the *obtaining data controller* is identifiable, the identifiable data controller standing proxy for all the data subjects who contributed personal data used by the obtaining data controller to represent *their* interests. In our opinion, this is necessary to take proper account of the theoretical aspects of the right to privacy because the view of what constitutes private personal data that best fits Article 8(1) ECHR is not data obtained from an identifiable person but data that is so related to a person that use of it is use of that person (in impinging on that person's self-image) whether or not that person is identifiable. However, from a purely practical point of view, it will be at least necessary (whether or not Recital 26 is given a narrow or a broad interpretation) for the fair processing provisions of Articles 10 and 11 to be interpreted so as to require data controllers to inform the data subjects of any anticipated anonymisation and the consequences of this for the ability of the data subject to control subsequent use of data rendered anonymous.

In the *Source Informatics* case, the UK Court of Appeal noted that anonymisation could be contrary to the data subject's interests in cases where anonymisation would be incompatible with the purposes for which the data was obtained (e.g., where it was obtained for the treatment of patients who still need that treatment).[21] Our analysis goes much further. Legal guidance from the UK Information Commission, which is the supervisory authority for the Data Protection Act 1998 states that anonymised data should be used wherever possible.[22] If the recommendation is for securely coded data, we agree. However, if it is for personal data to be rendered genuinely anonymous, we cannot agree, for this will have the effect of making it impossible to comply with the principles of protection in cases where the principles should (and do in theory) still apply.

NOTES

1. Recital 11 states that the principles of protection
   > give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

   On this basis, the principles of protection are the general rules on the lawfulness of processing laid down in Articles 5 to 21 of the Directive plus the requirement on Member States to provide judicial remedies, liability and sanctions (Articles 22 to 24). However, it is arguable that they include the rules on the transfer of personal data to third countries (Articles 25 and 26) (which the UK Data Protection Act 1998 treats as its eighth data protection principle).
2. According to paragraph 28 of the Explanatory Report to the Council of Europe Convention (with reference to Article 2(a) of that Convention's definition of "personal data")
   > "Identifiable persons" means a person who can be easily identified: it does not cover identification of persons by means of very sophisticated methods.

   However, because the Directive amplifies this Convention, it is not clear to what extent this applies to the Directive.
3. Article 10 requires controllers who obtain personal data from the data subject to inform the data subject of, *inter alia*, the purposes of intended processing of the data. Article 11.1 requires controllers who obtain personal data from a source other than the data subject to provide the data subject with essentially the same information as required by Article 10. Articles 7 and 8 lay down criteria for legitimate processing of personal data and sensitive personal data respectively.
4. See, e.g., the position taken by the UK Court of Appeal in *R v Department of Health, ex parte Source Informatics Ltd.* [2001] 1 All ER 786, especially at 799, which concerned a scenario essentially the same as scenario (2). The Court's basic reasoning is indicated below.
5. The ECHR has persuasive force in the context of EC law. One must also bear in mind that, according to Article 1.1 of the Directive, the Directive's object is to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data", with Recital 10 reminding us that the right to privacy is recognised both in Article 8 ECHR and in the general principles of EC law.
6. The UK Data Protection Act 1998, s.1(2)(b), states that, "unless the context otherwise requires", "'using' . . . in relation to personal data, includes using . . . the information contained in the data." When the context might require otherwise is not explained. In principle, this should be when the context is such that the use will not involve a threat to the data subject's right to privacy and other fundamental rights and freedoms, or when it is impossible to comply with the principles of protection in relation to the use of the information contained in the data (e.g., where the non-personal information to be used is contained in personal data but the data controller has no possible way of linking back to the personal data *even via* the data controller who originally obtained the personal data) *provided that* this has not come about through any failure of the user to comply with the principles of protection in relation to the personal data (see the final section of this paper for an explanation).
7. The UK Data Protection Act 1998, s.1(1), however, has it that the data is personal if the data subject can be identified directly by anyone or indirectly only by the data controller. It is arguable that this does not correctly implement the Directive.

8. The UK Data Protection Act 1998, s.1(2)(b), states that, "unless the context otherwise requires", "'disclosing' . . . in relation to personal data, includes disclosing . . . the information contained in the data."

   The document, *Data Protection Act 1998: Legal Guidance*, from the UK Information Commissioner (2001) states (at page 14, paragraph 2.2.5) that whether information is personal data in the hands of a person to whom the information is disclosed depends on whether *this* person can identify the data subject directly or with the help of information likely to come into the hands of *this* person. We do not agree. This is because, where *A* can still identify the data subject, *B* (who cannot identify the data subject) is using what is personal data given to *A* for specified purposes (if *A* has complied with the Act). If *B's* use is not subject to these purposes then *A* can get round having to comply with the principles of protection simply by getting *B* to process for other purposes.
9. In support of this, it should be noted that Article 14(b) requires the data subject to be informed not only of processing for purposes of direct marketing that the data controller who obtains the data anticipates undertaking, but whenever the data controller anticipates the data *being processed* for this purpose (unless the data controller informs the data subject of such use before it occurs).

   It is, of interest, therefore, that Mr. Justice Maurice Kay in *R on the Application of Brian Reid Beetson Robertson & City of Wakefield Metropolitan Council & Secretary of State for the Home Department*, 16 November 2001 (Case No. CO/284/2001 in the High Court, Queen's Bench Division (paragraphs 22–23), in order to reconcile the Directive with s.11(1) of the UK Data Protection Act 1998, which states

   > An individual is entitled at any time . . . to require the data controller . . . to cease, or not to begin, processing for the purposes of direct marketing personal data in respect of which he is the data subject

   held that where persons in the position of *A* anticipate processing being carried out by those like *B*, this processing is to be considered processing carried out by *A*.
10. All of these considerations also apply to scenarios (1) and (2).
11. *R v Department of Health, ex parte Source Informatics Ltd.* [2001] 1 All ER 786. For a full critical commentary on this case see Deryck Beyleveld and Elise Histed, "Betrayal of Confidence in the Court of Appeal" (2000) *Medical Law International* 4:277–311.
12. "The European Convention on Human Rights and the Right to Respect for Private Life, the Home and Communications" in A. H. Robertson (ed.), *Privacy and Human Rights* (Manchester: Manchester University Press, 1973) 12–128 at 92
13. *Andre Deklerck v. Belgium*. Application No. 8307/78 DR21, 116.
14. "Personality and Privacy Under the European Convention on Human Rights" *British Yearbook of International Law* LXI (1990) 175–197 at 196.
15. In our opinion, a person who obtains data in personal form but does not inform the data subject of processing for purpose X may not, without special legal exemption, process the data for this purpose if this processing was anticipated. Article 10 requires those who obtain data in personal form to inform of the purposes of the processing, etc. Recitals 39 and 40 reveal that this information is also to be given in two other situations (unless this is impossible or involves disproportionate effort or a specific legal exemption is provided): (a) where the person who obtained the data from the data subject did not anticipate the processing (including disclosure to a third party); and (b) where the data was not obtained from the data subject (this situation being covered by Article 11). From this, it follows that use for what were *anticipated* purposes about which the data subject was not at the time of obtaining

informed is prohibited (unless Member States provide a special legal exemption, which may only be provided for the purposes set out in Article 13) unless the data subject is informed before the processing begins. If the purposes were *unanticipated*, and the data subject cannot be informed or this would involve disproportionate effort, the exemption provided is still subject to provision of appropriate safeguards.

In relation to this, we also suggest that the test of whether or not a purpose was anticipated needs to be the objective one of whether that purpose was *reasonably foreseeable*, simply because the subjective test of whether it was actually *anticipated* is almost impossible to verify and, consequently, provides inadequate protection for the data subject.

16. In relation to this, our general view is that *in situations where* information provision for *unanticipated* purposes would be impossible/involve disproportionate effort *and where* the processing concerned pursues a worthwhile objective and is not a matter of known moral or religious objection or public sensitivity, non-personal information may be processed without informing the data subject. However, this is a matter of exemption *within the* principles of protection, not a matter of non-application of the principles.

In any case, this hardly applies to processing for genetic research, because this and the activities that it nowadays routinely involves (such as patenting) are known matters of moral objection and public sensitivity.

17. In at least one specific case, we interpret the UK Data Protection Act 1998 as taking the view that processing of data extracted from personal data that is no longer personal data is subject to the principles of protection. S.55(1) of the Act provides that persons

> must not knowingly or recklessly, without the consent of the data controller—
> (a) obtain or disclose personal data or the information contained in personal data, or
> (b) procure the disclosure to another person of the information contained in the personal data

and s.55(4) provides that a person who sells personal data without the consent of the data controller is guilty of an offence. However, according to the second sub-paragraph of s.55(7), for the purposes of s.55(4), "personal data" not only includes information contained in personal data, but also "information extracted from personal data" regardless of the context. The difference between "information contained in personal data" and "information extracted from personal data" is not explained. We suggest that the former implies that the original data set still exists as personal data, whereas the latter does not—it might or it might not. That the s.55(7) provision makes s.55(4) apply regardless of context is implied by the first sub-paragraph of s.55(7), according to which s.1(2) (which specifies that disclosure of personal data includes disclosure of information contained in the data unless the context otherwise requires) does not apply to s.55. Thus, because s.55(1) itself refers to disclosure of information contained in personal data, the only part of s.1(2) that can be disapplied by s.55(7) is the proviso "unless the context otherwise requires".

This, in general terms, fits our analysis *if* the reason for these provisions is that (as Article 6(2) provides) the data controller is responsible for lawful and fair processing (which implies that processing should not be without the consent of the data controller).

18. Applicable principles include Articles 10 and 11 (re information provision to the data subject), Article 14 re objection to processing and to use for purposes of direct marketing, Articles 7 and 8 (legitimate processing). Article 12 (subject access, etc.)

remains applicable while the data controller retains the original data set in personal form and, arguably, might even remain applicable afterwards as the fact that it is not possible to identify the data subject from the data does not mean that the data controller would not know that data on a particular data subject had been used in compiling or other wise creating the non-personal data.

19. Non-objection to which is, in any case, tantamount to non-objection to use for any (legitimate) purpose.
20. *Gunnar Nilsson, Per Olav Hagelgren, Solweig Arrborn, Agriculture (Case C-162/97)*, judgment of November 19, 1998, paragraph 54 of the judgment. An exception to this would, however, surely be if the recitals correctly refer to Treaty provisions. In such a case, the Directive would, surely, have to be declared invalid. For a general discussion of the status of recitals in EC Directives, see Deryck Beyleveld "Why Recital 26 of the EC Directive on the Legal Protection of Biotechnological Inventions Should Be Implemented in National Law" (2000) *Intellectual Property Quarterly* 4:1–26.
21. [2000] 1 All ER 786, at 799.
22. *Data Protection Act 1998: Legal Guidance*, p.13 paragraph 2.2.5. Office of the Information Commissioner, 2001.